الترميز الدولي / ISSN (P) :2710-2653
ISSN (E) :2960-253X /
رقم الايداع الوطني / 2375 /2019

تاريخ استلام البحث : ٢٠٢٥/١١/٢٣
تاريخ قبول البحث : ٢٠٢٦/١/٢٦
تاريخ النشر : ٢٠٢٦/٣/٣٠

الذكاء الاصطناعي وتأثيره في استراتيجيات الأمن السيبراني:
دراسة تحليلية لنماذج مختارة

Artificial Intelligence and Its Impact on Cybersecurity Strategies: An Analytical Study of Selected Models

أ.م.د محمد ميسر فتحي
Assistant Professor Dr. Mohammed Myaser Fathi
جامعة الموصل – كلية اللوم السياسية - فرع العلاقات الدولية
University of Mosul College of Political Science - Branch of International Relations
mohamed-kamosh@uomosul.edu.iq
ORCID: 0000-0002-1796-4389

IRAQI
Academic Scientific Journals
https://iasj.rdd.eedu.iq/journals/journal/view/229

الملخص:

في مستهل مخلص البحث، شكل الذكاء الاصطناعي تعزيزاً وإضافةً نوعيةً ومهمةً للأمن والقوة السيبرانية، إذ يساهم في دعم الإنتاجية وتحليل البيانات وأتمتة وإكتشاف التهديدات والإستجابة لها، مما يقلل العبء على المحللين البشريين، فضلاً عن ذلك تعمل خوارزميات التعلم الآلي للذكاء بتحليل حركة مرور الشبكة واكتشاف الحالات الشاذة والاستجابة للتهديدات في الوقت الفعلي، ما يضمن دفاعات أسرع وأكثر دقة، كما يتيح الذكاء الاصطناعي تطوير استراتيجيات هجومية ودفاعية سيبرانية مستمرة وقابلة للتكيف تساهم في تعزيز تدابير الأمن السيبراني لاسيما فيما يتعلق بجدران الحماية وأنظمة الكشف عن التسلل وأمان نقطة النهاية، هذا من جهه.

ومن جهةً ثانية نجد أن الهكرز والقراصنة وجدوا طرقًا لتوظيفه في أعمال التصيّد الاحتيالي، وإنشاء البرمجيات الخبيثة، واكتشاف الثغرات في الأنظمة، فضلاً عن ما تستطيع فعله هذه الأدوات من تحليل كميات هائلة من البيانات بسرعة لتحديد نقاط الضعف المحتملة في الشبكات، وبذلك يعدّ الذكاء الاصطناعي سلاح ذو حدين فهو يعزز الأمن السيبراني واختراقه تبعاً لقدرة القوى والفواعل الدولية وطريقة توظيفه، وهو مازاد من حدة التنافس والصراع السيبراني فضلاً عن سباق التسلح المعزز بالقوة السيبرانية والذكاء الاصطناعي.

الكلمات المفتاحية: الذكاء الإصطناعي، تقنيات الذكاء الاصطناعي، استراتيجيات الأمن السيبراني، الصراع السيبراني الإيراني–(الإسرائيلي).

Abstract:

Artificial intelligence has formed an important enhancement and addition to security and cyber power, as it contributes to supporting productivity, data analysis, automation, threat detection, and response, reducing the burden on human analysts. In addition, intelligent machine learning algorithms analyze network traffic, detect anomalies, and respond to threats in real time, ensuring faster and more accurate defenses.

Artificial intelligence also enables the development of continuous, adaptable cyber offensive and defensive strategies that enhance cybersecurity measures, especially in firewalls, intrusion detection systems, and endpoint security, on the one hand. On the other hand, we find that hackers and hackers have found ways to employ it in phishing, creating malware, discovering vulnerabilities in systems, as well as what these tools can do from analyzing huge amounts of data quickly to identify potential vulnerabilities in networks, and thus artificial intelligence is a double-edged sword as it enhances cybersecurity and its penetration depending on the ability of international forces and actors and the way it is employed, which increases the intensity of competition and cyber conflict as well as the arms race enhanced by cyber power and artificial intelligence.

Keywords: Artificial Intelligence, Artificial Intelligence Technologies, Cybersecurity Strategies, Iranian-(Israeli) Cyber Conflict.

المقدمة:

بادئً ذي بدء، أدت الثورة الرقمية عالمياً الى ارتفاع التهديدات السيبرانية لأمن المجتمعات، لاسيما مع التطور الهائل في قطاع التكنولوجيا لاسيما تقنيات وبرامج الذكاء الاصطناعي، إذ أصبحت العلاقة معقدة بين الذكاء الاصطناعي والأمن السيبراني، إذ يتم استغلال هذه التكنولوجيا المعاصره لاختراق المؤسسات والشركات الحكومية وغير الحكومية، سواء من قبل الافراد والهكرز والجماعات المتطرفة أو القوى الدوليه أثناء فترات التوترات والأزمات السياسية، كما يتم توظيف الذكاء الاصطناعي أيضاً كأداة متطورة لمواجهة هذه التهديدات السيبرانية وتوفير حماية أكبر، وزيادة قدرات الدول والفواعل الأمنية، الامر الذي يحتم على الدول والقوى والفواعل العالمية حول العالم، اتباع استراتيجية دمج أنظمة الذكاء الاصطناعي مع القدرات السيبرانية لتحقيق الأمن السيبراني.

وساهمت تقنيات الذكاء الاصطناعي والتعلم الآلي في تطوير استراتيجيات وأدوات الدفاع والهجوم السيبراني وجعلها أكثر قدرةً وفاعليةً، فضلاً عن ذلك تسمح الأدوات المعتمدة على الذكاء الاصطناعي بتحليل بيانات الأمن الضخمة بشكل آلي مصادر بيانات خارجية وحركة الشبكة لمطابقة الأنماط مع سلوكيات هجمات سابقة لإكتشاف التهديدات بسرعة ودقة أعلى بما يساعد فرق الأمن السيبراني من التصدي عبر استراتيجيات وتقنيات الذكاء المبتكره لاسيما الأنظمة الحديثة المعتمده على خوارزميات تعليم "السلوك الطبيعي" للشبكة والأجهزة، فتكتشف انحرافات غير مألوفة لاسيما (زيادات غير عادية في حركة البيانات) لتحديد الهجمات المجهولة أو الصفرية (Zero-day)، فضلاً عن حماية النقاط الطرفية عبر توظيف أدوات الحماية الذكية والتعلم الآلي لكشف البرمجيات الخبيثة على الحواسيب والخوادم عن طريق نماذج التعرف على بصمات السلوكيات المألوفة للبرمجيات الضارة، فضلاً عن تحليل السلوك المستخدم وتحسين الأمان، مما يوفر رؤية شاملة لحالات اختراق الأمن ويساهم في التنبؤ بالهجمات المستقبلية... وغيرها.

بالمقابل من ذلك، بات المهاجمون يستخدمون الذكاء الاصطناعي لتعزيز هجماتهم السيبرانية وجعلها أكثر دقة وقوة، ومن أشهر هذه الاستخدامات هي التزييف العميق (Deepfake)، إذ تُستَخدَم تقنيات توليد المحتوى الصناعي لإنتاج تسجيلات صوتية أو مقاطع فيديو مزيفة تبدو مألوفة وحقيقية،لاسيما ما أفادت IBM بأن المحتالين أرسلوا مكالمات مزيفة إلى عملاء بنوك كبرى باستخدام تقنية استنساخ الأصوات لتخطي إجراءات التحقق الصوتي وسرقة الأرصدة، فضلاً عن الهندسة الاجتماعية والتصيد الاحتيالي إذ يتم توليد رسائل احتيالية عالية التخصيص عبر تحليلات بيانات شخصية وعامة عن المستهدفين، فيصبح المحتوى أكثر إقناعاً ومهارة، كما يمكن للخوارزميات تعديل محتوى الرسالة ديناميكياً بناءً على سلوك المستهدف ما يزيد من فرص الإيقاع بالضحايا.

كما يتم الاعتماد على الذكاء الاصطناعي في تطوير البرمجيات الخبيثة، إذ يعمل المهاجمون على إنشاء برمجيات خبيثة تتكيف ذاتياً (Polymorphic Malware)، إذ تعمل تلك الخوارزمية بتغيير بصمتها التوقيعية باستمرار كي

تتجنب الاكتشاف بواسطة برامج مكافحة الفيروسات التقليدية، وبذلك أصبح بالإمكان توليد سلالات جديدة من البرمجيات الضارة في مدة زمنية قصيرة جداً لاتتجاوز خمس عشرة ثانية تقريباً بتوظيف تقنيات الذكاء الاصطناعي.

اهمية البحث:

تنبع أهمية هذا البحث من تناوله موضوعًا حيويًا يواكب التحولات العلمية والعملية في المجال محل الدراسة.ويسهم في إثراء الأدبيات الأكاديمية من خلال تقديم إطار تحليلي يساعد على فهم أبعاد الظاهرة المدروسة.كما تبرز أهميته في دعم صانعي القرار والباحثين بنتائج يمكن الإفادة منها عمليًا. ويساعد البحث في تشخيص التحديات القائمة واقتراح حلول أو تصورات قابلة للتطبيق. فضلاً عن ذلك، يفتح آفاقًا لدراسات مستقبلية تعمّق البحث في الموضوع نفسه.

إشكالية البحث:

وتنبثق الإشكالية مما يحمله الذكاء الاصطناعي من وجهين متضادين فهو من جهة يوفر استراتيجيات وتقنيات دفاعية تعزز الامن السيبراني ومن جهة ثانية يعمل على تعزيز قدرات المهاجمين والهكرز في برمجة التقنيات الهجومية واختراق الدفاعات السيبرانية.

فرضية البحث:

تنطلق الفرضية من وجود علاقة طردية بين الذكاء الاصطناعي واستراتيجيات الامن السيبراني في محورين أو اتجاهين متضادين؛ فالاتجاه الأول ان الذكاء يساهم في تعزيز استراتيجيات الأمن السيبراني بينما الاتجاه الثاني نجد إن الذكاء الاصطناعي يساهم في اختراق وفشل استراتيجيات الأمن السيبراني... وهذا بطبيعة الحال يعتمد على مدى القوة والقدرة التي تمتلكها فواعل الأمن السيبراني وكيفية توظيفها أما في الاتجاه الإيجابي أو في الاتجاه السلبي.

منهجية البحث:

كما اعتمدت الدراسة على المنهج الوصفي التحليلي والمنهج الوظيفي لاستعراض آليات عمل خوارزميات التعلم الآلي في صد الهجمات، ومقابلتها بالتقنيات الهجومية الحديثة لاسيما "التزييف العميق" و"التصيد الاحتيالي الذكي" فضلاً عن تطبيق المنهج الاستقرائي لاثبات صحة الفرضية.

المحور الأول

تطور الذكاء الاصطناعي ومفهومه وخصائصه ومفكروه

يُعد الذكاء الاصطناعي مجالاً متداخلاً ومعقداً ينتج عن تقاطع علوم الحاسوب، والفلسفة، وعلم النفس المعرفي والسلوكي وعلم الالات الاكترونية، وهو لا يقتصر عن كونه تقنية، بل هو مجال علمي متخصص يهدف إلى محاكاة وتطوير القدرات العقل البشري عبر توظيف الآلات، ويعدّ أحد فروع علوم الكمبيوتر، مهمته هي إنشاء آلات

والبرامج التي تستطيع القيام بالمهام التي تحتاج إلى ذكاءً بشريًا لاسيما في مجال فهم اللغة الطبيعية والتعرف على الصور وإتخاذ القرارات.. ومن هذا المنطلق سنحلل المفهوم والمنطلقات الفكرية للذكاء الاصطناعي وفق التقسيم الآتي:

أولاً: مفهوم الذكاء الاصطناعي

بالرغم من تعدد التعاريف، إلا أن الصياغة العلمية الأكثر دقة للذكاء الاصطناعي تتبنى منظور "الأنظمة العاقلة" (Rational Agents) ووفقاً لذالك يعرف الذكاء الاصطناعي بانه "دراسة وتصميم العملاء الأذكياء (Intelligent Agents)؛ إذ يُعرف العميل الذكي "بأنه نظام يتلقى مدخلات من بيئته، ويتخذ الإجراءات التي تزيد من فرص نجاحه في تحقيق هدف معين"، بعبارة أخرى، هو "العلم الذي يُعنى بكيفية جعل الآلات تؤدي وظائف تتطلب ذكاءً عند قيام البشر بها لاسيما (الإدراك، والاستدلال، والتعلم، وحل المشكلات)" وغالباً ما يتم تصنيف الذكاء الاصطناعي بأربعة محاور رئيسة هي: التفكير مثل البشر في استخدام العلوم والمعارف، والتفكير بعقلانية باستخدام المنطق الرياضي، والتصرف مثل البشر فهو يتمكن من اجتياز اختبار تورينج (Turing Test)، فضلاً عن التصرف بعقلانية كونه يمتلك سلوكاً موجهاً نحو الهدف لتحقيق أفضل نتيجة متوقعة. (محمد ٢٠٢١)

ولابد من الإشارة الى إن الذكاء الاصطناعي (AI) يعدّ مصطلح واسع يُستخدم لوصف الآلات أو أجهزة الكمبيوتر التي تستخدم خوارزميات التعلم الآلي، والشبكات العصبية، والتقنيات المتقدمة الأخرى لمحاكاة كيفية عمل الدماغ البشري، تحاكي هذه الآلات القدرات المعرفية البشرية للتخطيط والاستنتاج وحل المشكلات وتنفيذ المهام المعقدة والتعلم من خبرة المعالجات السابقة. (Goel 2021)

على المستوى التطوري نجد إن فكرة توظيف ذكاء اصطناعي لتعزيز الأمن السيبراني موجودة منذ أواخر الثمانينيات على الأقل، إذ تطور الأمن السيبراني باستخدام الذكاء الاصطناعي الطريقة التي تتبعها الفواعل والقوى الدولية في تحديد التهديدات الإلكترونية والحد من تداعياتها، ويشمل ذلك استخدام الأدوات والتقنيات المدعومة بالذكاء (AI) من أجل:- (العتيبي ٢٠٢١)

-تحديد الهجمات الإلكترونية وانتهاكات البيانات والهجمات الإلكترونية والتنبؤ بها والدفاع، فضلاً عن العثور على الفجوات ونقاط الضعف في دفاعات الأمن السيبراني والقضاء عليها

-أتمتة أدوات وحلول اكتشاف التهديد والاستجابة لها

-زيادة الوصول إلى استخبارات التهديدات وفعاليتها، وتعزيز ودعم إدارة التهديدات السيبرانية

ثانياً: خصائص وأدوات الذكاء الاصطناعي ومفكروه:

وبطبيعة الحال فالذكاء الاصطناعي يتميز بقدرات متقدمة تمكنه من أداء المهام المعقدة، ويمكن تحليل أبرز هذه الخصائص فيما يلي:- (الشمري ٢٠٢١)

– القدرة على التعلم والتكيف (Learning and Adaptation): وهذه الميزه الأبرز، إذ تمكن أنظمة الذكاء الاصطناعي، لاسيما عبر التعلم الآلي لاستخلاص الأنماط والقواعد من مجموعات البيانات دون الحاجة إلى برمجة صريحة لكل قاعدة ويتضمن ذلك التعلم تحت الإشراف، والتعلم غير المراقب، والتعلم المعزز.

– الاستدلال وإتخاذ القرار (Reasoning and Decision Making): تشمل القدرة على توظيف القواعد والمنطق (سواء المنطق الاستنتاجي أو الاستقرائي) لمعالجة المعلومات المتاحة والوصول إلى استنتاجات جديدة أو إختيار المسار الأفضل للعمل في ضوء حالة عدم اليقين.

– الإدراك والاستقبال (Perception): قدرة النظام على تفسير المدخلات الحسية لاسيما (الصوت،والصور،والفيديو) القادمة من البيئة الخارجية، ويشمل ذلك مجالات لاسيما الرؤية الحاسوبية (Computer Vision) ومعالجة الإشارات الصوتية.

– معالجة اللغة الطبيعية والتوليد (Natural Language Processing – NLP): ويعمل ذلك نحو تمكين الآلة من فهم اللغة البشرية (نص أو نطق)، وتحليلها، وفي الأداء المتقدم، توليد لغة بشرية متماسكة وذات مغزى.

– حل المشكلات (Problems Solving): ويم ذلك بتطبيق خوارزميات البحث والاستدلال والتحليل للعثور على تسلسل الإجراءات والانطلاق نحو الهدف المنشودة، كما في أنظمة التخطيط والروبوتات.

وعلى المستوى التطويري ظهر عدة مفكرين ساهموا في تطوير مجال الذكاء الاصطناعي، ومن أبرزهم نذكر منهم، آلان تورينج (Alan Turing) ١٩١٢–١٩٥٤ وهو مؤسس المجال النظري فقد طرح "اختبار تورينج" عام ١٩٥٠ والموسومة "Computing Machinery and Intelligence"، بوصفه معياراً فلسفياً لتحديد ما إذا كانت الآلة قادرة على إظهار سلوك ذكي معادل للذكاء البشري، وأيضاً وفي هذا الصدد قدم جون مكارثي (John McCarthy) ١٩٢٧–٢٠١١ مصطلح "الذكاء الاصطناعي" في مؤتمر دارتموث الأكاديمي عام ١٩٥٦ الذي يُعد نقطة الانطلاق لهذا المجال، كما اخترع لغة البرمجة LISP، التي ساهمت في تطوير أبحاث الذكاء الاصطناعي. (Turing 1950)

كما شارك العالم مارفن مينسكي (Marvin Minsky) ١٩٢٧–٢٠١٦ –الذي يعد رائد الشبكات العصبية– في تأسيس معمل الذكاء الاصطناعي في معهد ماساتشوستس للتكنولوجيا (MIT)، وركزت أعماله المبكرة على الشبكات العصبية، لكنه اشتهر لاحقاً بعمله في "مجتمع العقل" بوصفه انموذج نظري يعد الذكاء بأنه نتاج تفاعل العديد من "العملاء" البسيطة. فضلاً عن ماقدمه المفكر هربرت سايمون ١٩١٦–٢٠٠١ (Herbert A. Simon) عن النمذجة المعرفية، إذ كان من أوائل المنظرين الذين طبقوا الذكاء الاصطناعي على حل المشكلات البشرية المعقدة، وقد شارك في تطوير برامج مثل "Logic Theorist" و"General Problem Solver". (Minsky 2025)

وفي إطار ترابط العلاقة بين الذكاء الاصطناعي والامن السيبراني، نجد أن الأمن السيبراني يعدّ عملية تكنو–أمنية تهدف إلى حماية أنظمة وشبكات الكمبيوتر المتصلة بالإنترنت من الهجمات الرقمية والاختراقات أو التدمير أو التعطيل الذي يضم عديداً من البيانات التي يمكن استخدامها في الذكاء الاصطناعي، فضلاً عن ذلك هناك علاقة وثيقة بين الذكاء الاصطناعي والأمن الالكتروني والسيبراني، إذ يتم تطوير أنظمة الذكاء الاصطناعي التي يمكن استخدامها لتعزيز الأمن السيبراني، إلى جانب تنفيذ تدابير أمنية لحماية أنظمة الذكاء الاصطناعي من الاختراق أو التلاعب، وتزايد الجرائم لاسيما سرقة البيانات والتصيد الاحتيالي. (Carter 2019)

واستخلاصاً لما سبق نجد إن القوى الدولية والفواعل ذات القوة السيبرانية لجأت إلى توظيف وسائل عدة لمكافحة تلك التهديدات، إذ تعمل فرق الأمن السيبراني المؤهلة المجهزة بأحدث التقنيات ومنها تقنية الذكاء الاصطناعي، التي تساعد على الكشف السريع عن الأنشطة الضارة ومواجهتها، كما تقدم الحمايه للشبكات من تلك الهجمات، فضلاً عن ذلك يعمل الذكاء الاصطناعي في مجال الأمن السيبراني على إنشاء تطبيقات آمنة بشكل افتراضي، تقضي على نقاط الضعف وتزيد من الدقة في اكتشاف المشكلات وتسريع الأداء السيبراني، وأتمتة آليات الاستجابة، مما يعزز من البنية التحتية لأمن الدول والفواعل من المؤسسات والشركات سيبرانياً.

المحور الثاني

أدوات وتقنيات الذكاء الاصطناعي وتأثيرها في استراتيجيات الامن السيبراني

لابد من التأكيد على إن دخول الذكاء الاصطناعي في مجال الأمن السيبراني بقوة يهدف لدعم الإنتاجية وتحليل البيانات وتعزيز الامن السيبراني، لكن القراصنة والهكرز وجدو طرقاً لتوظيفه في أعمال التصيّد الاحتيالي، وإنشاء البرمجيات الخبيثة، واكتشاف الثغرات في الأنظمة الأمنية وبرامج حمايتها، وفي تقرير صادر عن شركة (رادوير) يؤكد أن أدوات الذكاء الاصطناعي تُستخدم اليوم لكتابة رسائل احتيال مقنعة يصعب تمييزها عن الرسائل الحقيقية، ولإنتاج برامج ضارة تستطيع تجاوز أنظمة الحماية التقليدية. كما تستطيع هذه الأدوات تحليل كميات هائلة من البيانات بسرعة لتحديد نقاط الضعف المحتملة في شبكات الامن السيبراني.ومما تقدم عرضه نستعرض الأدوات والتقنيات الذكية التي توظف في مجاليّ تعزيز وتهديد الأمن السيبراني في نقطتين مع التركيز على الاستراتيجيات السيبرانية والتقنيات الذكية التي تدعمها وفق الاتي:

أولاً: أدوات الذكاء الاصطناعي التي تهدد استراتيجيات الأمن السيبراني: ضمن إطار الدمج بين تقنيات الذكاء الاصطناعي واستراتيجيات الامن السيبراني ظهر لدينا مانطلق عليه تسمية "الذكاء الاصطناعي العدائي" الذي يمكن الفواعل اليبرانيين من مهاجمة أنظمة الدفاع السيبرانية عبر أدوات الذكاء الاصطناعي، عن طريق "تسميم" بيانات التدريب أو خداع النماذج، وبناءً على ما تقدم يمكننا أن نستعرض أبرز أنواع تهديدات الذكاء الاصطناعي لاستراتيجيات الامن السيبراني، وفق الاتي:– (غنام ٢٠٢١) (العتيبي ٢٠٢١) (محمد ٢٠٢١)

- استراتيجية الهجمات الموجهة (Targeted Attacks): تعد الهجمات الموجهة من أخطر أنواع الهجمات السيبرانية، حيث يستهدف المهاجمون مؤسسات محددة لأغراض معينة، مثل سرقة البيانات الحساسة أو تعطيل الخدمات الأساسية. يعتمد المهاجمون على جمع المعلومات التفصيلية عن الهدف واستخدام أساليب متقدمة لاسيما الهندسة الاجتماعية.
- استراتيجية البرمجيات الخبيثة: تشمل البرمجيات الخبيثة العديد من الأشكال مثل الفيروسات، وبرامج الفدية (Ransomware)، وأحصنة طروادة (Trojans)، ومن الممكن أن تسبب هذه البرمجيات سرقة البيانات أو تعطيل الأنظمة، مما ينتج عنها خسائر مالية كبيرة وتأثيرات سلبية على سمعة المؤسسات والدول.
- استراتيجية الهجمات التصيدية عبر الإنترنت (Phishing Attacks): تزداد الهجمات التصيدية، حيث يقوم المهاجمون بإرسال رسائل بريد إلكتروني أو نصوص مزيفة تبدو مشروعة لكنها تهدف إلى سرقة بيانات الدخول أو المعلومات الشخصية، وتزداد خطورة هذا النوع من الهجمات عندما يتم استهداف الموظفين الرئيسيين.
- استراتيجية الاختراقات: تتعرض غالبية المؤسسات بشكل متزايد لاختراقات البيانات، حيث يتمكن المهاجمون من الوصول إلى الأنظمة وسرقة كميات كبيرة من البيانات الحساسة، وهذه الاختراقات قد تكون نتيجة لضعف في البنية التحتية الأمنية أو نتيجة لعدم تحديث الأنظمة بشكل منتظم.
- استراتيجية هجمات البنية التحتية السيبرانية: وتستهدف بعض الهجمات السيبرانية البنية التحتية الأساسية مثل شبكات الكهرباء والمياه والاتصالات. وهذه الهجمات قد تؤدي إلى توقف الخدمات الأساسية وتسبب أضرارًا جسيمة على المستوى الوطني.
- استراتيجية الانترنت المظلم ومنتديات القرصنة: ظهرت نماذج القرصنة (FraudGPT– WormGPT) عام ٢٠٢٣ وإنتشرت بشكل أوسع في ٢٠٢٤، إذ اخذ يعتمد عليها المهاجمون في كتابة رسائل احتيال إلكترونية وإنشاء أكواد خبيثة تساعد في تنفيذ هجمات واكتشاف الثغرات، كما يستخدم (Worm GPT) انموذجًا شبيهاً بـ (GPT–J) مدرَّبًا على بيانات البرامج الضارة، فيما عُرض منصة (Fraud GPT) خدمة اشتراك توليّدية لوثائق مالية مزيفة وبرمجيات خبيثة وصفحات تصيّد، فضلاً عن منصة التي ظهرت في ٢٠٢٥ وهي (Xanthorox –Xenware) وأصبحت بديل أقوى المنصات والبرمجيات السابقة كونها تعمل وفق نماذج لغوية خاصة وبنية مكوّنة من وحدات صغيرة لتوليد الأكواد واستغلال الثغرات وتحليل البيانات، كما يدمج تقنيات الصوت والصورة لهجمات أكثر تعقيداً، وتجعل الهجمات أسرع وأكثر مرونة؛ إذ انها لا تتبع أنماطاً ثابتة بل تغيّر استراتيجياتها وتكتيكاتها أثناء الهجوم، ما يعقّد عملية اكتشافها. (Gupta 2024)

وفقًا لتقرير صادر عن شركة"Palo Alto Networks Unit 42 التي تروج لمنتديات الويب المظلم وتستخدم نماذج ذكاء اصطناعي المعدلة ومفتوحة المصدر ومخصصة كمساعدين للقرصنة، التي تُباع غالبًا عبر اشتراكات شهرية أو سنوية".

لاشك ان هذا الواقع يؤشر قلقاً متزايداً لدى خبراء الأمن ففي دراسة لشركة "Absolute Security " كشفت أن أكثر من نصف مسؤولي أمن المعلومات (٥٤ %) يشعرون بأن فرقهم غير مستعدة للتعامل مع تهديدات الذكاء الاصطناعي وبيّنت الدراسة أن (٤٦ %) منهم يرون أن الذكاء الاصطناعي يمثل خطراً أكبر مما يقدّم من منفعة، وأن ٣٩ % أوقفوا استخدامه خوفاً من التعرض لاختراقات، وان هناك إمكانية لاستغلال تكنولوجيا الأمن السيبراني المعزز بالذكاء الاصطناعي من قبل المجرمين الإلكترونيين الذين تم تصميمها لوقفهم، إذ يمكن للهكرز إدخال محتوى ضار في بيانات ذكاء اصطناعي أو التلاعب بخوارزميات (AI) لاختراق الدفاعات الأمنية السيبرانية، ويمكنهم أيضًا استخدام (AI) لمحاولة التهرب من الكشف أو العثور على نقاط الضعف في أنظمة أمان المؤسسة واستغلالها، كما يشمل ذلك استخدام ذكاء اصطناعي (AI) لإنشاء صور ومقاطع فيديو مزيفة، أو خداع الموظفين للكشف عن معلومات حساسة أو مسجلة الملكية، أو اختراق كلمات المرور وضوابط الوصول الخاصة بالمؤسسة. (محمود ٢٠٢٥)

ومما تقدم وفي إطار التحليل نستنبط إن ظهور هذه الأدوات يوضح كيف أن الذكاء الاصطناعي يعمل على "تخفيض حاجز المهارة المطلوب للجريمة السيبرانية"، مما يسمح لمزيد من الأفراد–الهكرز بشن هجمات متطورة – التي كانت سابقاً حكرًا على المتسللين ذوي الخبرة العالية– باستخدام الذكاء الاصطناعي على مواقع اكثر أمناً.

ثانياً: أدوات الذكاء الاصطناعي التي تعزز استراتيجيات الأمن السيبراني: إذ يوفر الأمن السيبراني المعزز بقدرات الذكاء الاصطناعي عديداً من الايجابيات المتقدمة مقارنة باستراتيجيات الأمن السيبراني التقليدية، لاسيما استراتيجية استباقية للأمن السيبراني والمخاطر المتوقعة في المستقبل المنظور، فضلاً عن معالجة البيانات الكبيرة بما يساهم في اكتشاف التهديد والاستجابة لها بشكل أسرع وأكثر دقة، كذلك تحديد الحالات غير المتعادة، والاستجابة للعلامات الأولى للمخاطر أو الهجمات المحتملة في الوقت الفعلي، فضلاً عن تحليل حركة المرور على الشبكة وسلوكيات الموظفين وتقارير الأنشطة، بما في ذلك حركة مرور البيانات على الشبكة والمستخدمين، وسجلات الأمن والأنشطة.

وعلى خلاف ذلك فأنه يتجاوز مهام الأمان الروتينية المؤتمتة عبر أتمتة تحليلات السجلات وعمليات فحص الثغرات الأمنية وغيرها من وظائف الأمان التقليدية السابقة، عبر ما تقدمه أدوات الذكاء من تحرر فرق الأمان لتركيز وقتها وجهودها ومواردها على مهام استراتيجية عالية المستوى، والتقليل من تقاطع البيانات السلبية الرائفة والإيجابية الخادعة يساعد على تحقيق الدقة الأكبر للأمن السيبراني بمنع مراكز العمليات الأمنية (SOCs) من الارتباك بسبب التقارير غير ذات الصلة أو الزائفة. (محمد ٢٠٢١)

ولابد من التأكيد على أنه يساهم في التنبؤ بالهجمات السيبرانية المستقبلية والتخطيط لها – وذلك عن طريق تحديد الهجمات السابقة والتعلم منها الذي يمكن لتقنيات الذكاء الاصطناعي والتنبؤ بالتهديدات الجديدة وتوقعها، وإتخاذ خطوات استباقية من المخاطر الأمنية ونقاط الضعف قبل استغلالها، ومساعدة المؤسسات على البقاء على اطلاع

بأحدث الأساليب والتقنيات والإجراءات (TTPs) التي يستخدمها الهاكرز الإلكترونيون، فضلاً عن توفير الجهد والوقت والمال على المدى الطويل عبر تقليل عدد الاختراقات والهجمات الأمنية، بما يساعد المؤسسات على حماية بياناتها وحماية سمعتها وتقليل تكلفة المعالجات والتعافي من الهجمات السيبرانية بشكل واسع. (A. Goel 2021)
فضلاً عن ذلك يدعم الذكاء الاصطناعي إتخاذ القرار (Decision Support) فهو يوفر تقنيات متقدمة وأدوات تحليلية تساعد فرق الأمن السيبراني في إتخاذ قرارات مبنية على بيانات دقيقة وموثوقة. ويمكن الاستفادة من هذه التقنيات في تحديد أولويات التهديدات وتخصيص الموارد بشكل فعال للتعامل معها.
وبطبيعة الحال، فإن توظيف "الذكاء الاصطناعي في منظومة الدفاع السيبراني الوطنية للدول لم يعد خياراً ترفياً، بل أصبح ضرورة استراتيجية تهدف إلى بناء قدرات دفاعية استباقية قادرة على التنبؤ بالهجمات وتحليلها وصدها بشكل آلي، مما يعزز من مناعة البنى التحتية الحيوية ويحفظ الأمن القومي وفق استراتيجيات متعددة هدفها الأساسي استخدام قدرة الذكاء الاصطناعي على تحليل كميات هائلة من البيانات بسرعة ودقة تفوق القدرات البشرية، وذلك لأتمتة عمليات الدفاع، وتسريع الاستجابة، واكتشاف الأنماط الخبيثة المعقدة"، وتقسيم هذه الاستراتيجيات إلى أربعة محاور رئيسة وهي:-

- **استراتيجية الاستخبارات التنبؤية للتهديدات (Predictive Threat Intelligence)**

تنطلق هذه الاستراتيجية من التركيز على توظيف الذكاء الاصطناعي لتحديد "ما هي الهجمات التي قد نواجهها في المستقبل؟" إذ ان تقنيات التعلم الآلي تحولاً جذرياً من الأساليب التقليدية القائمة على التوقيعات إلى دفاع استباقي وتكيفي أكثر، قادر على تحديد التهديدات غير المرئية سابقاً، لم يعد الهدف الاستراتيجي يقتصر على حظر البرامج الضارة المعروفة فحسب، بل يشمل فهم السلوكيات الخبيثة وتوقعها، ويتم ذلك وفق عدة خطوات ومرتكزات أهمها الاتي: (Apruzzese 2020)

أ- التحليل التنبؤي للمخاطر (Predictive Risk Analysis): تستخدم خوارزميات تعلم الآلة لتحليل بيانات الهجمات السابقة من جميع أنحاء العالم، فضلاً عن تحليل "الويب المظلم" ومنتديات القراصنة، وتحديد التكتيكات والتقنيات والإجراءات (TTPs) التي يستخدمها المهاجمون، وتوقع أنواع الهجمات المستقبلية الأكثر احتمالاً لاسيما هجمات الفدية، التصيد الاحتيالي الموجه، والقطاعات المستهدفة".

ب- تحديد أولويات الثغرات الأمنية (Vulnerability Prioritization): تقوم المؤسسات باكتشاف آلاف الثغرات الأمنية، ولكن لا يمكن معالجتها جميعًا في وقت واحد حيث يوظف الذكاء الاصطناعي بيانات حول استغلال الثغرات في العالم الحقيقي، لتحديد الثغرات الأكثر خطورة والتي يُحتمل أن يستغلها المهاجمون، وبذلك فان "الذكاء الاصطناعي يُغيّر والتعلّم الآلي نموذج الأمن السيبراني من الاستجابة التفاعلية للحوادث إلى البحث الاستباقي عن التهديدات والتنبؤ بها. يُمكّن هذا التحوّل الاستراتيجي المؤسسات من التحرّك "قبل وقوع الكارثة" – أي التحرّك قبل نجاح الهجوم". (Spring 2021)

- استراتيجية الدفاع والمنع الاستباقي (Proactive Defense and Prevention): تركز هذه الاستراتيجية على منع الهجمات عبر أنظمة دفاع ذكية، وترتكز على الاتي:- (الشمري ٢٠٢١)

أ- أنظمة كشف ومنع التسلل من الجيل التالي (NGIPS): إذ تستخدم نماذج تعلم الآلة لتحليل حركة مرور عبر الشبكة في الوقت الفعلي ومقارنتها بأنماط الهجمات المعروفة والجديدة مما يمكنها من حظر البرمجيات الخبيثة وهجمات "Zero-Day" (الهجمات التي تستغل ثغرات غير معروفة) قبل دخولها إلى الشبكة.

ب- كشف التصيد الاحتيالي (Phishing Detection): وتُستخدم تقنيات معالجة اللغات الطبيعية (NLP) لتحليل محتوى رسائل البريد الإلكتروني، والتحقق من الروابط، وتحليل أسلوب الكتابة لتحديد رسائل التصيد الاحتيالي بدقة عالية، حتى لو كانت تستخدم أساليب جديدة.

ج- تحليل سلوك المستخدم والكيان (UEBA): وهنا يقوم الذكاء الاصطناعي بإنشاء "خط أساس" للسلوك الطبيعي لكل مستخدم وجهاز على الشبكة مثل (أوقات الدخول، الملفات التي يتم الوصول إليها، كمية البيانات المنقولة) وعند حدوث أي انحراف عن هذا السلوك الطبيعي على سبيل المثال يقوم موظف يقوم بتنزيل كمية هائلة من البيانات في وقت متأخر من الليل، عندها يعمل النظام على إطلاق تنبيه، مما يساعد في كشف التهديدات الداخلية أو الحسابات المخترقة. (Gartner 2021)

د- نهج أمني متعدد الطبقات: يؤدي الدمج بين الذكاء الاصطناعي والتدابير الأمنية السيبرانية إلى إنشاء نظام دفاع قوي ومتعدد الطبقات، يعزز الامن فحتى في حالة اختراق طبقة واحدة ، لا يزال بإمكان الطبقة الأخرى توفير الحماية.

هـ- برامج تدريب وتوعية الموظفين: يظل الخطأ البشري أحد أكبر مخاطر الأمن السيبراني، فالعمل على تدريب الموظفين على التعرف على التهديدات والاستجابة لها ، مثل هجمات التصيد الاحتيالي، أمرا ضروريا للدفاع القوي.

و- تحسين الدفاعات السيبرانية (Enhanced Cyber Defense): إذ يُساهم الذكاء الاصطناعي في تحسين دفاعات المؤسسات من خلال تقديم توصيات مستمرة لتحديث الأنظمة الأمنية. يعتمد ذلك على التحليل المستمر للبيانات والتعلم من الهجمات السابقة لتطوير استراتيجيات أكثر فعالية.

التنبؤ بالتهديدات المستقبلية (Threat Prediction): ويساعد الذكاء الاصطناعي في التنبؤ بالتهديدات المستقبلية بناءً على تحليل البيانات التاريخية والاتجاهات الحالية، وهذا التنبؤ يمكّن المؤسسات من الاستعداد بشكل أفضل واتخاذ تدابير وقائية تقلل من مخاطر الهجمات، وبالتالي تساعد المؤسسات على الحفاظ على استمرارية أعمالها والحفاظ على أداء كفاءتها التشغيلية.

- استراتيجية الكشف والتحليل في الوقت الفعلي (Real-Time Detection): وتتمحور هذه الاستراتيجية على اكتشاف الهجمات التي تمكنت من تجاوز خطوط الدفاع الأولى عبر عدة مراحل هي:- (عبدالله ٢٠٢٠)

أ- كشف السلوك غير الطبيعي والشاذ: وتعدّ هذه القوة الحقيقية للذكاء الاصطناعي، بدلاً من البحث عن تهديدات معروفة فقط، يبحث الذكاء الاصطناعي عن أي سلوك "غير طبيعي" أو "شاذ" في الشبكة ليمكنها من اكتشاف الهجمات الجديدة أو التهديدات المتقدمة والمستمرة التي تتخفى داخل الشبكة لفترات طويلة.

ب- تحليل حركة المرور المشفرة: يعتمد الهكرز على التشفير لإخفاء أنشطتهم، بينما يمكن لنماذج الذكاء الاصطناعي تحليل "البيانات الوصفية" لحركة المرور المشفرة (مثل حجم الحزم وتوقيتها) دون الحاجة لفك تشفيرها، لتحديد التهديدات. (Mansted 2019)

- استراتيجية الاستجابة الآلية والحوكمة (Automated Incident Response): وتهدف إلى تقليل الوقت بين اكتشاف الهجوم واحتوائه (MTTR – Mean Time to Respond) وذلك عبر التقنيات الاتية:

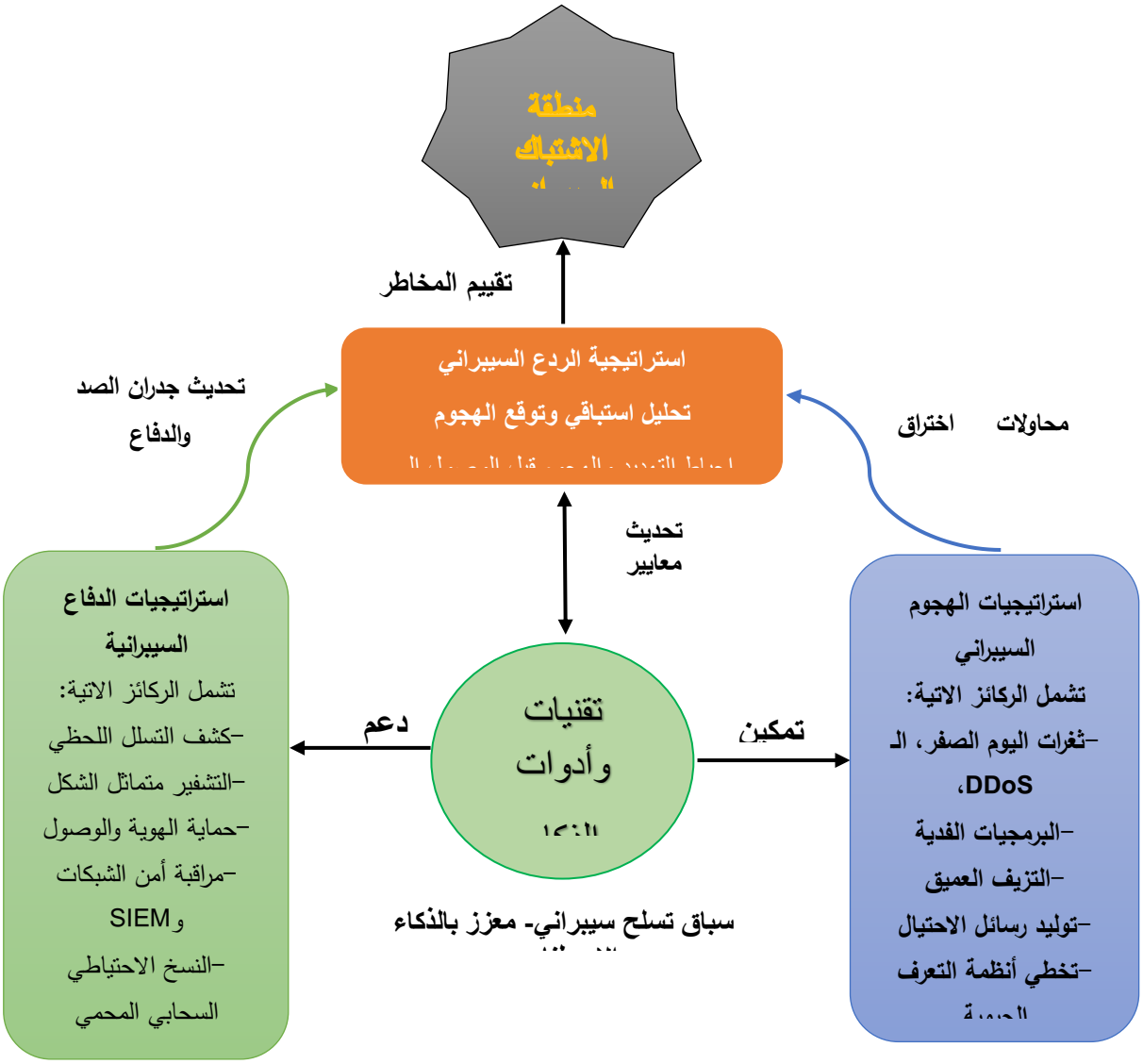
أ- الأتمتة والاستجابة المنسقة للأمن (SOAR): عندما يكتشف نظام مدعوم بالذكاء الاصطناعي تهديدًا، يمكنه تنفيذ "كتيبات لعب" (Playbooks) مُعدة مسبقًا بشكل آلي، ومنها (عزل جهاز مصاب عن الشبكة لمنع انتشار البرمجية الخبيثة، وحظر عنوان IP المهاجم على جدار الحماية، وتعطيل حساب مستخدم مخترق). (Chapple 2022)

ب- الصيد الاستباقي للتهديدات (Threat Hunting): وينطلق الذكاء الاصطناعي بمساعدة المبرمجين عن طريق تزويدهم ببيانات ورؤى حول الأنشطة المشبوهة التي قد لا تكون تهديداً مؤكداً، مما يسمح لهم بالتحقيق بشكل أعمق واكتشاف الهجمات الكامنة. (Husák 2019)

ج- استراتيجيات إدارة المخاطر السيبرانية والاستجابة الاستباقية: تعد معالجة الثغرات الأمنية بشكل استباقي أمراً أساسيا لتقليل التعرض. يمكن أن يساعد الذكاء الاصطناعي في تحديد نقاط الضعف في الشبكة والتوصية بخطوات المعالجة ، مما يضمن دفاعا قويا ضد الهجمات المحتملة، ويضمن إطار الاستجابة الاستباقية والسريعة لاحتواء التهديدات والمخاطر الإلكترونية والتعافي منها بسرعة، يمكن أن يلعب الذكاء الاصطناعي دورا رئيساً في أتمتة هذه العمليات واحكامها. (لاحظ الشكل رقم ١).

الشكل رقم –١–

علاقة التكامل بين استراتيجيات الدفاع والهجوم السيبرانية وتقنيات الذكاء



المخطط من أعداد الباحث.

وفي ضوء التحليل الاستراتيجي للشكل أعلاه، نجد انه هناك تنوع كبير في تقنيات الذكاء الاصطناعي التي تدعم استراتيجيات الأمن السيبراني (الهجومية والدفاعية والردع)، ويمثل الشكل انموذجاً لـ "المباراة الصفرية" (Zero–sum Game) بين طرفين فاعلين في الفضاء السيبراني بين الاستراتيجية الهجومية ولاستراتيجية الدفاعية حيث يتحول هذا الصراع إلى معركة خوارزمية تتسم بالسرعة الفائقة والقدرة على التكيف اللحظي. ولابد من التأكيد على تحول الاستراتيجيات الهجومية من "الهجمات التقليدية" إلى "الهجمات التوليدية" بدعم الذكاء الاصطناعي .

في المقابل من ذلك، تتبنى الفواعل استراتيجية "الدفاع النشط" (Active Defense) التي لا تنتظر وقوع التهديدبل تعتمد على تقنيات الذكاء الاصطناعي وكشف الشذوذ السلوكي والعزل الذاتي والتشافي والتشفير العصبي لصد الهجمات وفي حال فشلها يتم الانتقال في مستوى التصعيد الى استراتيجية الردع االسيبراني والاستجابة الالية لمنع الهجوم وفي حال فشل الردع ينتقل مستوى الصراح الى "ساحة الاشتباك" ويعتمد على قدرة الفواعل في توفير الحماية المطلقة او النسبية للامن السيبراني المعزز بالذكاء وتفعيل الهجوم الكامل ضد الطرف الاخر.

وفي الوقت نفسه تعمل التغذية الراجعة (Feedback Loop) بعد كل هجوم فاشل بتزود قاعدة بيانات المدافع لجعله أقوى وفق آلية التعلم الذاتي والتوليدي لاكتشاف ثغرات جديد والهجوم عليها، فضلاً عن ذلك ان كل تصدٍ ناجح يجبر المهاجم على ابتكار ثغرة من "اليوم صفر" (Zero-day)، وبناءً على ما تقدم لابد التحول من "الدفاع الساكن" إلى "الدفاع التنبؤي" لمواجهة تطور الذكاء الاصطناعي الهجومي.

المحور الثالث

استراتيجيات الأمن السيبراني المعززه بالذكاء الاصطناعي: ايران و(إسرائيل) انموذجاً

وفي ضوء استراتيجيات الأمن السيبراني المعززه بالذكاء الاصطناعي الذي اصبح سلاح ذو حدين، إذ تم توظيفه في استراتيجيات الأمن السيبراني الهجومية (بالتهديد) والدفاعية (بالحمايه)، وانطلاقاً من ذلك نستعرض هذه الاستراتيجيات مع نماذج متنوعه في الجدول المدرج ثم ننتقل للتركيز على مؤسسات واستراتيجيات الأمن السيبراني الإيرانية و(الاسرئيلية) وتطورات الصراع بينهما.

أولاً : مؤسسات واستراتيجيات الامن السيبراني الإيرانية المرتكزه على الذكاء الاصطناعي

❖ **المؤسسات:** تمتلك إيران العديد من المؤسسات والأذرع التي تعزز من قدراتها السيبرانية تؤازرها إستراتيجية سيبرانية لها أبعاد هجومية، وأخرى دفاعية، وفق الآتي: (البيضاني، ٢٠٢٥)

– المجلس الأعلى للفضاء السيبراني (SCC): يعدّ هيئة حكومية لادارة وتوجيه السياسات والاستراتيجيات الوطنية للأمن السيبراني وتأسس في عام ٢٠١٢ بوصفه هيئة رئيسة تسعى للسيطرة على مجالات الإنترنت والفضاء السيبراني والذكاء الاصطناعي ويرأسها الرئيس الإيراني، ويهدف إلى تنسيق العمليات السيبرانية الدفاعية والهجومية ، وتطوير استراتيجيات الأمن السيبراني، وحماية البنية التحتية الحيوية للبلاد من التهديدات الخارجية.

– قوات الباسيج السيبراني (مجلس الباسيج السيبراني): وتركز هدفها بالدرجة الأولى على تنظيم دعاية موالية لإيران في المجال السيبراني، وتطوير قدرات متقدمة في هذا المجال، والدفاع عن رموز الدولة ضد المعارضين، سواء في شبكات التواصل الاجتماعي أو في المدونات الإلكترونية، وقد حصلت قوات الباسيج على دور مهم في المجال السيبراني في الحرب الناعمة الإيرانية، وهي تقوم بهجمات سيبرانية أقل تطورًا، حيث إنها تضم عناصر غير محترفين يعملون تحت إشراف خبراء في الحرس الثوري يطلق عليهم اسم "كوماندوس الحرب السيبرانية"، مثل

عمليات التسلل واختراق حسابات البريد الإلكتروني والمواقع الإلكترونية للناشطين والمعارضة السياسية، كما تعمل على تعزيز حملات التأثير عبر نشر محتوى الكتروني يتماشى مع قيم الثورة.

– المركز الوطني للفضاء السيبراني: ويرتبط المركز بالمجلس الأعلى للفضاء السيبراني وتهتم لجنة التنسيق الوطنية فيه إلى حد كبير بمحتوى المعلومات وتطوير ضوابط أمن شبكات الإنترنت الداخلية.

– فيلق الحرس الثوري: ايضاً يشرف على الأنشطة السيبرانية الهجومية، وتتبعه كذلك منظمة الحرب السيبرانية والدفاع السيبراني، التي توفر دورات تدريبية في مجال الدفاعات السيبرانية، وتمنع الوصول إلى المحتوى والاتصالات عبر الإنترنت مع مراقبة هذه الاتصالات.

– الجيش السيبراني الإيراني: يتشكل من خبراء ومتسللين محترفين ومن ذوي المهارة العالية في مجال التكنولوجيا والذكاء الاصطناعي لاختراق مواقع العدو، وتحويل حركة المرور في الإنترنت، واختراق مواقع وسائل الإعلام الحكومية الأجنبية ومنصات التواصل الاجتماعي.

– قيادة الدفاع السيبراني: وتُعرف هذه المؤسسة باسم المقر السيبراني في الجيش الإيراني أيضًا، وتقوم بعمليات هجومية سيبرانية، وتطوير إستراتيجيات ضد تهديدات الفضاء السيبراني، جنبا إلى جنب مع مجلس الباسيج السيبراني، وتتألف على نحو رئيس من أفراد عسكريين، وتخضع لإشراف هيئة الأركان العامة للقوات المسلحة.

– مركز أمن المعلومات: الذي يعمل تحت سلطة وزارة الاتصالات وتكنولوجيا المعلومات، ويتمثل دوره الرئيس في الاستجابة المباشرة للطوارئ في حالة وقوع هجمات سيبرانية.

❖ **الاستراتيجيات:** ساهم الذكاء الاصطناعي في تطور استراتيجيات الأمن السيبراني الإيرانية، مقسمة حسب مجالات التأثير، وهي:

– استراتيجية التصيد والهندسة الاجتماعية الهجومية: إذ "أحدث الذكاء الاصطناعي نقلة نوعية في القدرة السيبرانية الإيرانية في شن هجمات معقدة تعتمد على الخداع، "تقوم الأجهزة بصياغة رسائل بريد إلكتروني ومستندات مقنعة للغاية باستخدام أدوات الذكاء الاصطناعي المتقدمة، لتقليد شخصيات بارزة في صناعة الأمن والأوساط الأكاديمية، وهذا أدى الى رفع من مستوى التطور والموثوقية في عمليات التصيد الاحتيالي الموجه، كما سمح الذكاء الاصطناعي التوليدي للجهات الفاعلة بالتحرك بشكل أسرع وبحجم أكبر، مما جعل المهاجمين أكثر كفاءة في صياغة رسائل التصيد وتطوير البرمجيات." (Group 2024)

كما يشير الباحثون إلى أن الذكاء الاصطناعي ساعد القراصنة الإيرانيين في تجاوز عائق اللغة، عبر "استخدام نماذج لغوية كبيرة (LLMs) لصياغة رسائل تصيد احتيالي مقنعة للغاية، وإنشاء ملفات تعريف مزيفة، وإجراء استطلاع مفتوح المصدر، وبذلك ساهم الذكاء الاصطناعي في التقليل من الحواجز أمام الدخول، مما يسمح للمهاجمين بتوسيع نطاق عملياتهم بسرعة وكفاءة أكبر من أي وقت مضى". (Baram, AI and the evolution of state-sponsored cyber warfare: The case of Iran 2024)

ومن أمثلة ذلك ما قامت به إيران باستخدام الذكاء الاصطناعي التوليدي لإنتاج مقاطع فيديو وصور مزيفة عالية الدقة لإثارة الذعر في الداخل الإسرائيلي والمبالغة في حجم الأضرار العسكرية، إذ شهد الصراع بين إسرائيل وإيران في يونيو ٢٠٢٥ أول استخدام واسع النطاق ومنسق للتزييف العميق (Deepfakes) في حملات التضليل في زمن الحرب، ونشرت الشبكات المرتبطة بإيران مقاطع فيديو تم إنشاؤها بواسطة الذكاء الاصطناعي تدعي كذباً أنها تظهر دماراً هائلاً في مطار بن غوريون وتل أبيب بعد الهجمات الصاروخية، مستغلة أدوات (Google Veo) لإنتاج صور واقعية للغاية". (Hozint 2025)

– استراتيجية النفوذ والتضليل الإعلامي عالية المصداقية (Deepfakes و Fake News): تعد هذه الاستراتيجية الأكثر تأثراً بالذكاء الاصطناعي، إذ تستخدمه إيران لإنشاء محتوى ضخم وموجه للتأثير على الرأي العام العالمي، وقد "استخدمت الأجهزة السيبرانية الإيرانية نماذج الذكاء الاصطناعي لإنشاء مقالات طويلة وتعليقات عبر وسائل التواصل الاجتماعي... لقد أنشأوا شبكات من المواقع الإخبارية المزيفة التي تستخدم الذكاء الاصطناعي لسرقة المحتوى وإعادة صياغته لاستهداف الناخبين الأمريكيين برسائل مزيفه، وأصبحت ايران المستخدم الأكبر لعمليات التضليل بنسبة ٧٥% من الاستخدام المكتشف لأغراض التلاعب بالرأي العام وتكييف المحتوى لجمهور مختلف"، فضلاً عن ذلك تستخدم إيران الذكاء الاصطناعي لإنشاء مواقع إخبارية سرية لاسيما موقعي (Nio Thinker) و(Savannah Time) اللذين صُمما لجذب الجماهير من أطياف سياسية متعارضة". (Center 2025)

ومع التطور الخطير للحرب النفسية، اخترقت مجموعة "Handala" (المرتبطة بوزارة الاستخبارات الإيرانية) أنظمة النداء العام في رياض الأطفال في (إسرائيل) لبث أغاني مخيفة وتحذيرات، بالتزامن مع إرسال آلاف الرسائل النصية القصيرة (SMS) التي تهدد (الإسرائيليين). يشير المحللون إلى أن الأتمتة والذكاء الاصطناعي ساهما في توسيع نطاق هذه الهجمات لتشمل آلاف الأهداف في وقت واحد بدقة عالية". (Baram, AI and the evolution of state-sponsored cyber warfare: The case of Iran 2024)

– استراتيجية تعزيز القدرات الدفاعية غير المتكافأة: وتعمل على توظيف الذكاء الاصطناعي بوصفه أداة "مضاعفة للقوة السيبرانية" لتعويض الفجوة التكنولوجية وتعزيز السيطرة الداخلية، إذ "تنظر القيادة الإيرانية إلى الذكاء الاصطناعي كقوة رئيسة للأمن القومي... وتعمل على دمج الذكاء الاصطناعي في عملياتها السيبرانية، وتطوير العقيدة السيبرانية الهجومية والأنظمة والصناعية العسكرية، والبنية التحتية للمراقبة المحلية". (Tabatabai 2024) كما يتم دمج تقنيات الذكاء الاصطناعي في الأنظمة السيبرانية الدفاعية والهجومية لتعزيز قدرات الردع السيبراني وتشكيل تهديدات غير متكافئة ضد البنية التحتية الحيوية للخصوم، فضلاً عن تطوير خوارزميات قادرة على رصد الأنماط السلوكية للمعارضين وتحديد التهديدات السيبرانية. (Baram, AI and the evolution of state-sponsored cyber warfare: The case of Iran 2024)

فضلاً عن ذلك طورت مجموعة (Muddy Water) التابعة لوزارة الاستخبارات الإيرانية برمجيات خبيثة جديدة لاسيما (Muddy Viper) وتستخدم منطقاً برمجياً معقداً يحاكي "لعبة الثعبان" تعمل تأخير التنفيذ وخداع أنظمة الكشف المتقدمة، مستهدفة قطاعات الهندسة والحكومة المحلية في (إسرائيل).(News 2025)

وتمتلك إيران عدداً من الاستراتيجيات العسكرية المدعومه بالقوة السيبرانية والذكاء الاصطناعي والدمج بينهما بما يعزز أدائها الاستراتيجي حيال اعدائها، ومن أهمها الاتي:-

- استراتيجية "الاستهداف الحركي المعزز سيبرانياً" (Cyber-Enabled Kinetic Targeting): كما تشير أحدث التقارير الاستخباراتية إلى تغيير جذري في العقيدة العسكرية الإيرانية، إذ لم تعد الهجمات السيبرانية مجرد أداة للتجسس أو التخريب، بل أصبحت جزءً من "سلسلة القتل" (Kill Chain) لتوجيه الضربات الصاروخية بدقة، وتؤكد التقارير "أن مجموعات القرصنة المرتبطة بإيران، لاسيما مجموعة(Imperial Kitten)، لم تعد تكتفي بالتجسس الرقمي، بل تعمل على اختراق أنظمة المراقبة وكاميرات CCTV ومنتجات أنظمة التعريف الآلي (AIS) في السفن التجارية وجمع بيانات استهداف دقيقة في الوقت الفعلي، وتُستخدم هذه البيانات لتوجيه الصواريخ الباليستية والطائرات المسيرة بدقة عالية ضد أهداف اسرائيلية." (A. S. Intelligence 2025) كذلك وفي إطار عقيدة "الحرب الهجينة" توظف ايران الهجمات الإلكترونية لتعطيل رادارات الدفاع الجوي للخصم أو إرباك أنظمة القيادة والسيطرة قبل لحظات من شن هجوم صاروخي أو بطائرات مسيرة، مما يرفع من احتمالية نجاح الضربة." (Canetti 2025)

- استراتيجية الطائرات المسيرة الموجهة بالذكاء الاصطناعي (AI-Guided Suicide Drones): عملت ايران على تصنيع جيل جديد من المسيرات التي تعتمد على (الرؤية الحاسوبية) للعمل في بيئات التشويش الإلكتروني الكثيف(GPS-denied environments)، وتشير التقارير انه"تم العثور في أوكرانيا على حطام لنسخة جديدة من طائرة 'شاهد-١٣٦' (Shahed-136 MS) مزودة بمعالج 'Nvidia Jetson' ووحدة استهداف حرارية، يسمح هذا النظام للطائرة بالعمل كـ (صياد مستقل)، عن طريق الذكاء الاصطناعي للتعرف بصرياً على الأهداف وتعديل مساره في المرحلة النهائية من الطيران من دون وجود إشارات GPS، مما يجعل أنظمة التشويش التقليدية غير فعاله تجاهها. (Magazine 2025)، وفي هذا السياق "أعلن الحرس الثوري الإيراني عن تزويد طائراته المسيرة من طراز مهاجر-٦ (Mohajer-6) وأبابيل-٥ (Ababil-5) بصواريخ ذكية من نوع قائم وألماس تستخدم خوارزميات الذكاء الاصطناعي لـ (أطلق وانسَ) (Fire-and-forget)، مما يمكنها من تتبع الأهداف المتحركة بدقة عالية وتدميرها ذاتياً".

استراتيجية الصواريخ الفرط صوتية والمناورة الذكية (Hypersonic & AI-Maneuverability): وتركز إيران على تطوير هذه الصواريخ ودمج تقنيات الذكاء الاصطناعي للمناورة وتفادي أنظمة الدفاع الجوي المتقدمة مثل "القبة الحديدية" أو "مقلاع داوود" في (إسرائيل) لاسيما "صاروخ 'فتاح-٢' (Fattah-2) الفرط صوتي يمثل قفزة

نوعية، إذ انه يدمج نظام توجيه بالذكاء الاصطناعي في مرحلة الانقضاض النهائية ويساهم هذا النظام بدعم الصاروخ بتغيير مساره وزاوية الهجوم بسرعات تفوق (٥ ماخ) بناءً على رصد التهديدات الدفاعية في الوقت الفعلي، مما يجعل اعتراضه شبه مستحيل". (Baram, Iran's AI ambitions: From strategic goals to offensive capabilities 2025) وما يعزز ذلك ما"صرحبه قائد البحرية في الحرس الثوري، الأدميرال علي رضا تنغسيري، بأن جميع الصواريخ الجديدة التي يتجاوز مداها ١٠٠٠ كيلومتر، بما في ذلك صواريخ كروز البحرية، وهي مزودة بالذكاء الاصطناعي وتضمن دقة إصابة تصل إلى أقل من متر واحد". (C. S. Intelligence 2025, February 24)

ثانياً: مؤسسات واستراتيجيات الامن السيبراني (الاسرائيلية) المرتكزه على الذكاء الاصطناعي:

- **المؤسسات:** إذ ركزت (إسرائيل) على بناء قدرات دفاعية وهجومية متقدمة لتعزيز أمنها القومي، وتأسست القيادة السيبرانية الإسرائيلية (Cyber Command) عام ٢٠١٧ للإشراف على العمليات السيبرانية عبر المؤسسات السيبرانية الاتية:-

أ- الوحدات العسكرية المتخصصة كالوحدة (٨٢٠٠) التي تعد أهم وحدة استخبارات سيبرانية في الجيش (الإسرائيلي)، وهي مسؤولة عن جمع وتحليل المعلومات الإلكترونية، وتنفيذ عمليات هجومية ضد الخصوم والوحدة ٨١ المتخصصة في تطوير أدوات الهجوم السيبراني والذكاء الاصطناعي الأغراض عسكرية، (محسن ٢٠٢٥) وتُعد إحدى أقوى أذرع هيئة الاستخبارات (أمان)، ويمتد عملها إلى كل أنحاء العالم تقريبا إلا أنها تركز على مناطق المسؤولية أولا وهي: (غزة وجنوب لبنان والضفة الغربية و إيران والعراق واليمن)..، ونظرًا إلى ما تملكه من إمكانات وخبرات فأنها تستطيع تزويد المؤسسات (الإسرائيلية) الأمنية والعسكرية والسياسية والاقتصادية بتدفق متواصل من المعلومات اللازمة، بعد جمعها عبر اختراقات وعمليات تجسس واستخبارات سيبرانية موثوقه. (البيضاني ٢٠٢٥)

لاشك تمثل هذه الوحدة قاعدة تجسس سيبرانية (إسرائيلية) الأهم والأكبر ومقرها (منطقة النقب) وضمن قاطع القيادة الجنوبية للجيش الصهيوني، إذ تشمل:

- الطيف الهجومي للاستخدام العسكري والقدرات السيبرانية.
- التنصت على البث الإذاعي، والمكالمات الهاتفية، والفاكس ووسائط التواصل الاجتماعي بمختلف برامجها، البريد الإلكتروني في قارات آسيا وأفريقيا وأوروبا.
- قيادة أنظمة التتبع للشخصيات المطلوب تصفيتها أو استهدافها
- المساهمة بشكل فعال ومدروس في برامج التواصل الاجتماعي لأغراض متناقضة إما الكشف عن هويات المؤيدين للقضية الفلسطينية أو تجنيد العرب والفلسطينيين وغيرهم لصالح دعم الكيان.

كما تشير تقارير إلى أن الوحدة أدت دوراً مهماً في تعقب مواقع قيادات حركة "حماس" وعلماء الطاقة النووية في ايران، عبر استخدام أدوات تعتمد على تحليل الصوت، والتعرّف إلى الوجوه، ورصد اللغة العربية، فضلاً عن تطبيقات تعتمد على روبوتات المحادثة، وتظهر محاولة استهداف هذه الوحدة الأهمية المتزايدة للبنية المعلوماتية في (إسرائيل)، في ظل التحول المتسارع نحو الاعتماد على تقنيات الذكاء الاصطناعي في العمليات العسكرية، كما يكتسب هذا الهجوم بُعدا إضافيا في ضوء التعاون القائم بين الوحدة ٨٢٠٠ وعدد من شركات التكنولوجيا الكبرى مثل (مايكروسوفت) و(غوغل)، و(ميتا)، وهو تعاون يُنظر إليه بوصفه عنصرا ذا حساسية أمنية، وتشير التقديرات إلى أن الهجوم ربما استهدف إضعاف البنية التحتية الرقمية (الإسرائيلية)، أو كشف بعض الأساليب المستخدمة في إدارة العمليات، أو تحقيق نوع من الردع السيبراني المتبادل. (البيضاني ٢٠٢٥)

ب- الهيئة الوطنية للأمن السيبراني (INCD) التي تعمل على حماية البنية التحتية المدنية من الهجمات السيبرانية وتعزيز التعاون بين القطاعين العام والخاص، والمركز الوطني للسايبر (Cyber National Center) الذي يهدف إلى تطوير الأبحاث والابتكارات في مجال الأمن السيبراني. (محسن ٢٠٢٥)، علماً انه انشأ بعد أعلن رئيس الحكومة الإسرائيلية المجرم (بنيامين نتنياهو) في ١٨ أيار/ مايو ٢٠١١ عن إنشاء "هيئة السايبر الوطنية" وذكر أن الهدف الأساس لهذه الهيئة هو تعزيز قدرات إسرائيل الدفاعية عن أنظمة البنى التحتية الحيوية، من "هجمات إرهابية" في الفضاء الالكتروني، التي قد تقوم بها دول أجنبية أو "منظمات إرهابية"، ووفق ما ذكره، فإن الكيان الصهيوني مكشوف لهجمات في الفضاء السيبراني.

ويشير (شموئيل بن سيمان وايفن ودافيد) أنه علاوة على مهامها الدفاعية عن الفضاء السيبراني الإسرائيلي، فإن من مهام "هيئة السايبر الوطنية" تشجيع وتطوير شركات إسرائيلية مختصة في الدفاع، بغرض الحصول على جزء من سوق الفضاء الالكتروني الذي ينمو بسرعة كبيرة للغاية على الصعيد العالمي. (سيمان ٢٠١١) وإن يتلخص عملها بالاتي:

- تنسق جوانب الدفاع السيبراني المدني جميعاً، بدءً من الدفاع العملياتي إلى بناء القدرات التكنولوجية ومقترحات السياسة.
- تطوير الحلول السيبرانية المبتكرة والحلول التكنولوجية الاستشرافية،
- صياغة الإستراتيجيات والسياسات الوطنية والدولية.

جـ - التعاون مع القطاع الخاص: اذ تعتمد إسرائيل على التعاون الوثيق مع الشركات التكنولوجية الكبرى مثل (Check Point) و(NSO Group)، التي تطور أدوات سيبرانية متقدمة تستخدم في الأمن والدفاع والاستخبارات.

د- مديرية (C41) المعروفة أيضًا باسم C41 Corps، أي فيلق المعالجة من بعد تتمثل مهمتها في حماية البنية التحتية للاتصالات (الإسرائيلية) وأنظمة المعالجة في الجيش الإسرائيلي، علاوة على ذلك، تدعم المديرية تطوير "التكنولوجيا السيبرانية ذات الصلة"، وهي تتبع من الناحية التنظيمية مديرية خدمات الحاسوب المعروفة أيضًا باسم

Aka Atak، وقد تحولت مهمة C41 في الدفاع السيبراني نحو نهج "الدفاع النشط"، الذي يستلزم مجموعة من الهجمات الردعية والاستباقية.

هـ- القبة السيبرانية (Cyber Dome): تهدف إلى رصد الهجمات السيبرانية المحتملة والدفاع عن المرافق الحيوية للكيان، ولا سيما تلك التي تدار إلكترونيا، لغرض توفير الحماية المطلوبة لمختلف المرافق (الإسرائيلية)، من خلال آليات استباقية حول سبل السيطرة على استخدام الإنترنت على نطاق واسع في (إسرائيل) في مجالات الحياة جميعا. (البيضاني ٢٠٢٥)

ويبدو أن هناك ميلاً نحو مركزية مشهد الأمن السيبراني (الإسرائيلي) الذي كان لا مركزيا في ما سبق، ويكتمل الأمن السيبراني المدني بالدفاع السيبراني العسكري، الذي يقع تحت رعاية الجيش الصهيوني، وتتولى الوحدة ٨٢٠٠ في الجيش وكما بينا في أعلاه مسؤولية المهمات الهجومية، بينما يركز (فيلق المعالجة عن بعد C41) على التدابير الدفاعية . (البيضاني ٢٠٢٥)

❖ **الاستراتيجيات الإسرائيلية السيبرانية:** بناءً على التطورات المتسارعة اعتمدت (إسرائيل) استراتيجية الدفاع والهجوم السيبراني المدمج بالذكاء الاصطناعي، ومن أهمها ما يأتي:-

- استراتيجية "القبة السيبرانية" (Cyber Dome Strategy) وحماية البنية التحتية من الهجمات الإيرانية الضخمة، إذ "سرّعت إسرائيل نشر مبادرة 'القبة السيبرانية' (Cyber Dome)، التي تعدّ منصة مركزية تعتمد على الذكاء الاصطناعي التوليدي لتحليل مليارات الإشارات الرقمية في الوقت الفعلي وسجل هذا النظام نجحاً للتنبأ بالهجمات الإيرانية في تحديد واحتواء برمجيات خبيثة استهدفت شبكات الكهرباء والمياه الإسرائيلية قبل أن تتسبب في أي انقطاع للخدمة، وهو تحول من الدفاع التفاعلي إلى الدفاع التنبؤي". (Directorate 2025) (INCD)) 2025)

كما مكنت خوارزميات الذكاء الاصطناعي المدمجة في "مشروع نيمبوس (Project Nimbus) السحابي الحكومة الإسرائيلية" من استمرارية العمليات العسكرية والمدنية عبر بيئة مشفرة ومراقبة آلياً لاسيما أثناء الهجمات السيبرانية الإيرانية المكثفة ما أدى الى أحبط هجمات مجموعات القراصنة الإيرانية لمسح البيانات الحكومية الصهيونية، فضلاً عن ذلك تدخلت أنظمة "القبة السيبرانية" لعزل الأجهزة المصابة آلياً عن الشبكة المركزية دون تدخل بشري ماساعد في منع انهيار الانظامة الالكترونية. (Zilberstein 2025)

- استراتيجية أنظمة الاستهداف الهجومي (AI-Driven Targeting Systems): ان الأداء الاسرائيلي في الحرب الأخيرة، استخدم أنظمة مثيرة للجدل تعتمد على الذكاء الاصطناعي لتسريع وتيرة تحديد الأهداف العسكرية الإيرانية ووكلائها، مثل نظامي "الإنجيل" (The Gospel) و"لافندر" (Lavender). كما "أحدث الجيش الإسرائيلي تحولاً جذرياً في بنك الأهداف عبر نظام هبسورا (The Gospel)، الذي يعتمد التعلم الآلي لمعالجة

كميات كبيرة من البيانات الاستخباراتية، وتحديد مواقع مخازن الصواريخ ومراكز القيادة التابعة للحرس الثوري في سوريا ولبنان بدقة وسرعة تفوق القدرة البشرية، مما سمح بضرب مئات الأهداف الحيوية. (Davies 2024)

في ضوء المواجهة الاخيرة مع إيران، وظفت (إسرائيل) الذكاء الاصطناعي لدمج المعلومات الواردة من الأقمار الصناعية واعتراض الإشارات وبناء نماذج تخمينية ثلاثية الأبعاد للمنشآت الإيرانية تحت سطح الأرض ما ساهم في توجيه الهجمات السيبرانية والضربات الجوية الدقيقة لتعطيل خطوط إنتاج الطائرات المسيرة الإيرانية. (INSS)) 2025)

– استراتيجية الدفاع الجوي والصاروخي المعزز بالذكاء الاصطناعي: ان التحديات التي واجهتها أنظمة الدفاع الجوي الإسرائيلية عبر كم كبير ومختلط من الطائرات المسيرة والصواريخ الباليستية الإيرانية. دافعها الى تطوير خوارزميات الذكاء الاصطناعي لتؤدي دوراً حاسماً في بفرز الأهداف (Target Prioritization) في أجزاء من الثانية، إذ ميزت هذه الأنظمة بين الرؤوس الحربية الحقيقية والخداعية، فضلاً عن التنبئ بمسار "أسراب" المسيرات والعمل على توزيع مهام الاعتراض آلياً بين الطائرات المقاتلة ومنظومات الدفاع الأرضي وحسب مسار سقوطها المتوقع في المناطق الحيوية. (Rubin 2024)

– استراتيجية الحرب النفسية ومكافحة التضليل (Counter–Disinformation): فقد وظفت أدوات الذكاء في رصد وتحليل وكشف حملات التأثير الإيرانية الموجهة لتفتيت الجبهة الداخلية الإسرائيلية. ونشرت وزارة الخارجية الإسرائيلية والمؤسسات السيبرانية برامج ذكاء اصطناعي لرصد شبكات البوتات (Bots) الإيرانية عبر برامج التواصل الإجتماعي، كما إن تلك الأدوات لم تكتفِ بالحذف الآلي، بل قامت بتحليل السرديات والاشاعات المعادية وإنتاج محتوى مضاد (Counter–narratives) مدعوم بالحقائق وموجه لجمهور محدد في إيران والشرق الأوسط، في سابقة لاستخدام الذكاء الاصطناعي في الدبلوماسية الرقمية الهجومية. (Reporter 2025)

– استراتيجية "العمى السيبراني–الحركي" (Cyber–Kinetic Blinding): تستخدام هجمات سيبرانية دقيقة لتعطيل رادارات ودفاعات العدو الجوية قبل أجزاء من الثانية من تنفيذ الهجوم، وتجسد ذلك في الرد الصهيوني عبر استراتيجية تكنولوجيا معقدة ومتقدمة للتخفي (Stealth) بدأت بتحييد نظام الدفاع الجوي S–300 الذي يحمي منشأة نطنز النووية في أصفهان وتزامنه ذلك مع هجوم إلكترونية شل قدرة الرادار على الكشف، مما سمح لصاروخ موجه بدقة بتدمير الهدف دون أن يتم رصده. (Sanger 2024)

– استراتيجية "ساحة المعركة الرقمية الموحدة" (Digital Twin & Unified Battlefield): وترتكز هذه الاستراتيجية على بناء "توأم رقمي" (Digital Twin) لساحة المعركة، وربط القوات البرية والجوية والسيبرانية في شبكة واحدة مدعومة بالذكاء الاصطناعي في مشروع "Edge of Tomorrow" حيث يتم نقل المعلومات الاستخباراتية من الوحدات السيبرانية (Unit 8200) مباشرة إلى قمرة القيادة في طائرات F–35 والقوات البرية، كما

تسمح هذه الاستراتيجية بإغلاق دائرة الاستشعار إلى التنفيذ في ثوانٍ معدودة، وهو مامكنها من تدمير منصات إطلاق المسيرات الإيرانية قبل اطلاقها بناءً على تحليل بصماتهم الإلكترونية والحرارية أنياً. (Staff 2024)

وتعتمد القوة السيبرانية (الإسرائيلية) على استراتيجيات متعددة تطمح عبرها إلى تحقيق الامتداد الجيواستراتيجي للقوتها السيبرانية، لاسيما الاستراتيجية الدفاعية التي تعتمد على تطوير أنظمة حماية متقدمة لمنع الاختراقات والهجمات السيبرانية وتنفيذ تدريبات سنوية لمحاكاة الهجمات السيبرانية وتعزيز الجاهزية الإلكترونية وتعزيز التعاون الدولي في مجال الأمن السيبراني مع الولايات المتحدة ودول أوروبية، فضلاً عن الاستراتيجية الهجومية التي تشمل تنفيذ عمليات سيبرانية هجومية لتعطيل أنظمة الخصوم، كما حدث في الهجوم المشترك مع الولايات المتحدة باستخدام فيروس "ستوكسنت (Stuxnet) لتعطيل البرنامج النووي الإيراني عام ٢٠١٠ ، واستهداف البنية التحتية الإلكترونية لحركات المقاومة الفلسطينية وإيران لتعطيل أنظمتها المالية والعسكرية واستخدام البرمجيات الخبيثة وأدوات القرصنة لاستهداف شبكات الدول المعادية"، فضلا عن الاستراتيجية الاستخباراتية عبر توظيف الذكاء الاصطناعي وتحليل البيانات لتعقب الجماعات المسلحة والشبكات الإرهابية وتنفيذ عمليات تجسس إلكتروني لجمع معلومات عن الجهات المعادية واستخدام تقنيات التعلم الآلي والتعلم العميق وتحليل البيانات الضخمة لكشف المعلومات الأمنية. (محسن ٢٠٢٥)

وفي ضوء تحليل الاستراتيجيات تصاعدت الهجمات الإيرانية فمنذ اندلاع الحرب، شهدت إسرائيل زيادة بنسبة تزيد عن ١٠٠% في الهجمات السيبرانية وبمتوسط يتجاوز ٢,٠٠٠ هجمة أسبوعياً لكل منظمة، وهو ضعف المعدل العالمي. (Research 2024) كما شكلت الهجمات الإيرانية مايقارب (٧٥%) من جميع عمليات التأثير المدعومة بتقنيات الذكاء الاصطناعي، مستهدفة بشكل أساسي الرأي العام الإسرائيلي والعالمي. (G. T. Intelligence 2025)

وتيشر التقديرات إنها تمكنت من إحباط أكثر من (٨٠٠) هجمة سيبرانية كبرى (Potential Mega-Attacks) كانت تهدف لإحداث أضرار مادية جسيمة وذلك بفضل أنظمة الكشف المعتمدة على الذكاء الاصطناعي. (C. S. Intelligence 2025, February 24)، كما أدت الهجمات السيبرانية المنسوبة لمجموعة ' Predatory Sparrow' إلى تعطيل نحو (٧٠%) من محطات الوقود في جميع أنحاء إيران، في إطار استعراض قدرات الحرب السيبرانية-الفيزيائية. (Reuters 2024)

الخاتمة:

وخلاصة القول نجد إن الذكاء الاصطناعي أصبح عاملًا حاسماً في تعزيز الأمن السيبراني، إذ يوفر أدوات وتقنيات قادرة على مواجهة التهديدات المتطورة بسرعة وفعالية، بقدرته في الكشف الاستباقي عن التهديدات، والتحليل السلوكي المتقدم، والاستجابة التلقائية للحوادث، يلعب الذكاء الاصطناعي دورًا محوريًا في حماية البيانات والبنية التحتية من المخاطر السيبرانية والحد من آثارها السلبية على الأنظمة الرقمية الحيوية.

وبالرغم من ذلك، إن الاعتماد على الذكاء الاصطناعي في تعزيز استراتيجيات الأمن السيبراني ليس حلاً؛ إذأنه يتطلب تحقيق التكامل مع استراتيجيات بشرية وأدوات تقليدية لضمان نظام دفاع شامل ومُستدام للتعامل مع التحديات السيبرانية المتزايدة باستمرار.

ولاشك في ان ضمان مستقبل الأمن السيبراني لا يتحقق الا بالتكيف والتعاون المستمرين عبر دمج التدابير الاستباقية التي تعتمد على الذكاء الاصطناعي في مبتكرة للأمن السيبراني، بما يمكن للقوى والفواعل الاخرى الحفاظ على مرونتها ضد التهديدات المتطورة.

الاستنتاجات:-

- مكن الذكاء الاصطناعي من الكشف المبكر عن التهديدات، والاستجابة التلقائية، وتحليل السلوك، ما جعله يؤدي دوراً حيوياً لحماية البنية التحتية الرقمية والبيانات السرية، كما أن الفواعل التي تستثمر في هذه التقنيات ستحظى بقدرة أكبر على مواجهة تهديدات الأمن السيبراني المعقدة وضمان استمرارية الحماية في بيئة رقمية آمنة.
- ومع تطور المشهد الرقمي وتحسين الذكاء الاصطناعي وما يوفره من الفرص الهائلة للابتكار، واكتشاف التهديدات بشكل آلي فضلاً عن شبكات الشفاء الذاتي الامر الذي يمهد الطريق لظهور جيل جديد للأمن السيبراني.
- تعدّ استراتيجيات الأمن السيبراني المعززة بالذكاء الاصطناعي نقلة نوعية في استراتيجيات الهجوم والدفاع الرقمي، إذ تحولت من انموذج "رد الفعل" (Reactive) الذي يعتمد على اكتشاف الهجمات عند وقوعها، إلى انموذج "استباقي وتنبؤي" (Proactive & Predictive) يهدف إلى التنبؤ بالتهديدات ومنع تداعياتها.
- أن (إسرائيل) انتقلت من الاستخدام التقليدي للتكنولوجيا إلى "الشراكة مع تكنولوجيا الذكاء الاصطناعي وتقنياته"، إذ لم يعد الذكاء مجرد أداة مساعدة، بل أصبح "العقل المدبر" الذي يدير الهجمات والدفاعات الجوية والقصف الصاروخي عبر التشويش السيبراني.
- يؤكد غالبية الخبراء والمختصين أن استراتيجية الأمن السيبراني الإيرانية تطورت من الاعتماد على "الكمية" والهجمات التدميرية البسيطة، إلى استراتيجية تعتمد على "الجودة والكفاءة" المدعومة بالذكاء الاصطناعي.
- كما يمكننا الاستنتاج بأن استراتيجية إيران قد تطورت في اتجاهين رئيسين بفعل الذكاء الاصطناعي: لاسيما الكفاءة والاداء للانتقال من هجمات الحرمان من الخدمة (DDoS) البسيطة إلى هجمات الهندسة الاجتماعية المعقدة والمدعومة بـ LLMs، فضلاً عن حرب المعلومات بتوظيف الذكاء الاصطناعي لإنشاء جيوش سيبرانية ذات رد آلي قادرة على إغراق الفضاء الإعلامي بمعلومات موجهة بتكلفة منخفضة جداً.
- إن الاستراتيجية الإيرانية لعام ٢٠٢٥ اعتمدت مبدأ "التفوق غير المتماثل الذكي" (Smart Asymmetric Superiority)، الذي يرتكز على الدمج العملياتي بتوظيف القوة السيبرانية الحركية، فضلاً عن الاستقلال الذاتي لإطلاق وتوجه الاسلحة بجعل الصواريخ والمسيرات قادرة على "اتخاذ القرار الذاتي" في اللحظات الأخيرة لضمان دقة الإصابة رغم التشويش.

المصادر باللغة العربية:

١. البيضاني، حسن سلمان خليفة" .2025 .الحرب السيبرانية في المواجهة العسكرية الإيرانية (الإسرائيلية) ". *مجلة حمورابي* .45.
٢. خالد وليد محمود. ٢٠٢٥. *تقرير يكشف تهديدات غير مسبوقة للذكاء الاصطناعي*. ٢٥ ١٢. https://www.aljazeera.net/opinions/2025/12/20/.
٣. الشمري، خالد بن بندر" .2021 .استراتيجيات الدفاع السيبراني النشط المعتمدة على الذكاء الاصطناعي ". In *آفاق جديدة في الدراسات الأمنية* by ,تحرير سعد بن محمد الشهراني، ٢١٥-٢٤٠ .الرياض: جامعة نايف العربية للعلوم الأمنية.
٤. شموئيل ايفن ودافيد بن سيمان. ٢٠١١. *حرب الفضاء الالكتروني - تحديات على الصعيد العالمي والسياسي والتكنولوجي*. (إسرائيل): معهد دراسات الأمن القومي.
٥. عبير أسامة محمد. ٢٠٢١. *الذكاء الاصطناعي والأمن السيبراني*. القاهرة: المجموعة العربية للتدريب والنشر.
٦. علي عبدالله. ٢٠٢٠. *الأمن السيبراني والذكاء الاصطناعي: التحديات والفرص*. عمّان: دار اليازوري العلمية للنشر والتوزيع.
٧. غنام، شريف محمد .2021 .*جرائم الذكاء الاصطناعي* .الإسكندرية- مصر: دار الجامعة الجديدة.
٨. فهد بن دحيم العتيبي. ٢٠٢١. *الذكاء الاصطناعي والأمن السيبراني*. الرياض: مكتبة الملك فهد الوطنية.
٩. محسن، محمد معد" .2025 .القوة السيبرانية الإسرائيليةوتأثيرها على استراتيجيات القوى الإقليمية "*.المجلة العلمية لجهاز مكافحة الارهاب* .86-85 :9

المصادر باللغة الانكليزية:

1. Apruzzese, Giovanni, et al. 2020. "he Role of Machine Learning in Cybersecurity." *Digital Threats: Research and Practice* 1: 2.
2. Baram, G. 2024. " AI and the evolution of state-sponsored cyber warfare: The case of Iran." *Journal of Cyber Policy* 9 (2): 112-128.
3. Baram, G. 2025. *Iran's AI ambitions: From strategic goals to offensive capabilities.* Journal of Cyber Policy.
4. Canetti, D., & Dor, G. 2025. *From missiles to malware: Hybrid war is rewriting global security.* The Loop (ECPR).
5. Carter, Katherine Mansted and William A. 2019. *The Weaponization of Artificial Intelligence*. Washington: D.C.: Center for Strategic and International Studies (CSIS).
6. Center, Microsoft Threat Analysis. 2025. *Iran surges cyber-enabled influence operations in support of Hamas.* 11 2. https://blogs.microsoft.com.
7. Chapple, Mike, and David Seidl. 2022. "Cyberwarfare: The CISO's Guide to Building a Resilient Organization." *Hoboken, NJ: John Wiley & Sons* 118.
8. Davies, H., & McKernan, B. 2024. *The machine did it coldly': Israel used AI to identify targets in Gaza and beyond.* April 3. https://www.theguardian.com.
9. Directorate, Israel National Cyber. 2025. *Annual threat assessment: The rise of AI-driven defense mechanisms against state actors.* Israel: INCD Publications.
10. Gartner. 2021. *Market Guide for User and Entity Behavior Analytics.* Stamford: CT: Gartner.
11. Goel, Ankur. 2021. *Artificial Intelligence for Cybersecurity*. New York: New York Apress.

12. Goel, Ankur. 2021. *Artificial Intelligence for Cybersecurity.* New York: New York: Apress.
13. Group, Insikt. 2024. *The future of influence: AI-driven threat landscape.* Recorded Future.
14. Gupta, M., Akiri, C., Aryal, K., Parker, E., & Praharaj, L. 2024. *From ChatGPT to ThreatGPT: Impact of generative AI in cybersecurity and privacy.* IEEE Access. 11. https://doi.org/10.1109/ACCESS.2023.3300381.
15. Hozint. 2025. " The use of generative AI deepfakes in the Israel–Iran conflict." *Hozint Security Intelligence.*, July 2.
16. Husák, Martin, et al. 2019. "Survey of Attack Projection, Prediction, and Forecasting in Cyber Security." *Tutorials* (IEEE Communications Surveys) 1: 641.
17. Intelligence, Amazon Security. 2025. *Iran regime's cyber-kinetic warfare: A dangerous new front.* November 21. https://irannewsupdate.com.
18. Intelligence, Cyber Security. 2025, February 24. *Iran deploys AI-guided missiles & drones.* Cyber Security Intelligence.
19. Intelligence, Google Threat. 2025. *Tool of first resort: AI in information warfare.* Google : Google Cloud Security.
20. (INCD), Israel National Cyber Directorate. 2025. Report 2024-2025: AI-driven resilience in critical infrastructure. (Israel): INCD Publications.
21. (INSS), Institute for National Security Studies. 2025. *AI in warfare: Strategic implications of the Israel-Iran escalation.* Institute for National Security Studies-INSS.
22. Magazine, Defense. 2025. *First combat use of AI-guided Iranian Shahed drone alarms Ukraine.* Defense Magazine.
23. Mansted, Katherine and William A. Carter. 2019. *The Weaponization of Artificial Intelligence.* Washington: Center for Strategic and International Studies (CSIS).
24. Minsky, Marvin Lee. 2025. *Britannica Editors History.* https://www.britannica.com/biography/Marvin-Minsky.
25. News, The Hacker. 2025. *Iran-linked hackers hit Israeli sectors with new MuddyViper backdoor* (December).
26. Reporter, Fake. 2025. *Digital shield: Defending democracy against foreign AI influence operations.* FakeReporter Annual Report.
27. Research, Check Point. 2024 . *Cyber attack trends: 2024 mid-year report.* Check Point Software Technologies.
28. Reuters. 2024. *Software failure disrupts gas stations across Iran.* December 18.
29. Rubin, U. 2024. *The interplay of AI and missile defense: Analysis of the April and October exchanges.* Begin-Sadat Center for Strategic Studies (BESA).
30. Sanger, D. E., & Schmitt, E. 2024. *Israel's strike on Iran was limited but sent a clear signal of technological superiority.* April 20. https://www.nytimes.com.
31. Spring, Jonathan M. 2021. "Cybersecurity with Artificial Intelligence: A Five-Level Maturity Model." *IEEE Security & Privacy 19* 6: 32.
32. Staff, Jerusalem Post. 2024. *IDF reveals integration of AI into combat units for rapid target acquisition.* June 12. https://www.jpost.com.
33. Tabatabai, A. M. 2024. *Iran's digital repression strategy: AI and the future of authoritarian control.* Center for Strategic and International Studies (CSIS).

34. Turing, Alan M. 1950. *Computing Machinery and Intelligence. Mind.*
35. Zilberstein, S. 2025. "Cloud sovereignty and AI: Lessons from the Israel-Iran cyber conflict." *Journal of Strategic Security* 18 (1): 45-62.